the IG

FRAUD ALERT

November 2018

W-2 Phishing Scams

As the end of the year approaches and the tax season begins, the Internal Revenue Service (IRS) warns employers to stay alert against W-2 Form phishing scams. While phishing scams are generally widespread to target the most potential victims, W-2 phishing scams are more focused.

Criminals target large companies and organizations. The criminals identify their top executives and the personnel responsible for payroll and personal records. Once they are able to assume the email identity of top executives, the criminals send an e-mail to the unsuspecting payroll department requesting copies of employees W-2 forms.

W-2's contain employee names, addresses, Social Security numbers, income, and withholdings. This information allows criminals to file fraudulent tax returns and redirect the refunds to themselves. The refunds are redirected to criminals, and since the criminals use actual W-2 information, it is more difficult for the Internal Revenue Service to stop the criminals.

The criminals can also use W-2 information to apply for credit cards in the unsuspecting employee's name. When the credit card company verifies the information on the credit card application, it comes back as valid because the information was taken from the employee's actual W-2. Once criminals obtain a credit card, they can make purchases and take cash advances with the fraudulent credit card.

Another way for the criminals to profit from the W-2 information is to sell the employee information on the "dark web." Criminals are able to sell the W-2 information to other criminals who will continue to victimize the employee.

How to protect employees:

- Employees should file their tax returns as soon as possible so that the criminals do not have a chance to file a fraudulent return.
- Employers should have controls in place to ensure that employee information cannot be requested by a single individual without verifying the request.
- Employers should alert the IRS as soon as they become aware of the phishing scam so that the IRS can take steps to reduce the chances the employees will become victims.
- Employees should review their credit history regularly for unauthorized activity.

Sources: ***W-2 phishing scam targets consumers' tax refunds, Consumer Affairs***

For more information or to file a complaint, contact Pinellas County Consumer Protection at (727) 464-6200 or visit www.pinellascounty.org/consumer.

DIVISION OF INSPECTOR GENERAL
CLERK OF THE CIRCUIT COURT & COMPTROLLER
PINELLAS COUNTY, FLORIDA
35 Years of Improving Government
1983 - 2018

KEN BURKE
CLERK OF THE CIRCUIT COURT
AND COMPTROLLER

VOICE

You Have A VOICE Report Cybercrime

FRAUD ALERT

SIGN UP TODAY and receive free alerts when a document with your name is recorded in Official Records. Protect yourself from fraud. **CLICK HERE.**

GET IN TOUCH:

Write:
Public Integrity Unit
Division of Inspector General
Fraud Hotline
510 Bay Avenue
Clearwater, FL 33756

Call:
(727) 45FRAUD
(727) 453-7283
Fax:
(727) 464-8386
E-mail:
fraudhotline@mypinellasclerk.org
Internet:
www.mypinellasclerk.org
www.twitter.com/pinellasig
www.facebook.com/igpinellas

the IG

FRAUD ALERT